CLAIMS

1.   (Currently Amended) A method for transmitting data through a computer network, the computer network including a first computer and a second computer both having a message sequence number stored therein, the method comprising:

transmitting a message from the first computer to the second computer, the message including ~~containing~~ a message identifier, a user authentication portion comprising an encrypted message sequence number, and a data portion comprising encrypted data but not including user authentication data ~~from the first computer to the second computer~~;

decrypting the user authentication portion of the message ~~encrypted message sequence number~~ to authenticate the identity of the sending party who transmitted the message without decrypting the data portion of the message; and,

when the identity of the sending party is authenticated, the second computer initiating transmission of the message sequence number and the encrypted data to a third computer.

2.   (Original) The method of claim 1 wherein the message sequence number is incremented in both the first computer and the second computer for each subsequent message transmitted from the first computer to the second computer.

3.   (Original) The method of claim 1 wherein the message sequence number is initialized as a randomly generated number in one of the first and second computers.

4.   (Currently Amended) The method of claim 1 further comprising the third computer ~~step of~~ decrypting the ~~first~~ encrypted data transmitted by the first computer and received by the second computer ~~in the third computer~~ using the message sequence number.

2

5.   (Currently Amended) A computer network, comprising:

a first computer operably communicating with a second computer, both the first and second computers having a predetermined message sequence number stored therein;

a third computer operably communicating with the second computer;

the first computer configured to transmit a message containing a message identifier, a user authentication portion comprising an encrypted message sequence number, and a data portion comprising encrypted data but not including user authentication data to the second computer, the second computer configured to decrypt the ~~encrypted message sequence number~~ user authentication portion of the message to authenticate the identity of the sending party who transmitted the message without decrypting the data portion of the message; the second computer further configured to transmit the sequence number and the encrypted data to the third computer after the identity of the sending party is authenticated by the second computer.

6.   (Original) The computer network of claim 5 wherein the message sequence number is incremented in both the first computer and the second computer for each subsequent message transmitted from the first computer to the second computer.

7.   (Original) The computer network of claim 5 wherein the message sequence number is initialized as a randomly generated number in one of the first and second computers.

8.   (Currently Amended) The computer network of claim 5 wherein the third computer is further configured to decrypt the encrypted data transmitted by the first computer and received by the second computer using the message sequence number.